Open Network Architecture for Army Vehicle Electronics

Macam S Dattathreya

***Abstract*—The army vehicle electronics networking is complex and is receiving considerable attention in the concept of open and standard architecture. Electronic devices are from multiple vendors with unique interfaces. A successful battle depends on the effective interoperable communication between these devices. No commercial open architecture available to address interoperability, scalability, and security issues. Current standard network protocols, topologies, and bandwidth requirements are evaluated, and three architecture proposals are presented and evaluated. Hardware & software service oriented open network architecture for army vehicle electronics is presented. The latency, single point failure, scalability, security, and redundancy of the proposed architecture are evaluated. Initial evaluation has shown favorable results.**

***Index Terms*—Army vehicle network architecture, electronic network architecture, open architecture, vehicle architecture**

I. Introduction

ARMY vehicle electronics networking is complex and challenging due to vendor specific unique devices and its interfaces. Military vehicle require 100% network uptime and security, compliant with MILS (Multiple Independent Levels of Security), DODAF (Department of defense architecture framework), and DOD8500.2 standards. The network must reduce vehicle clutter; focus on saving Soldiers lives; minimum latency, and reduced logistics footprint. Battle requirements change frequently and vehicle electronics are added ad-hoc to the existing network. In this situation, in general, proprietary kit/appliqué vehicle electronics from various vendors are added ad-hoc to save time and cost. Interoperability, performance, and scalability analysis for this are significantly complicated and costly.

For this situation, author introduces open standard architecture approach which offers non proprietary solutions with good interoperability, security, scalability, performance benefits, and cost savings. Open standard architectures are public specifications, not requiring any subscriptions to use it or modify it. This allows anybody to design add on products to mature the technology and ultimately reduce the cost.

All current commercial network architectures are proprietary [8] and the army vehicles are showing considerable interest in utilizing open standards.

The author presents open standard architecture solution for solving complex army vehicle electronics networking. The solution consists of combined hardware and service oriented software for addressing networking complexities.

The author presents his solution details in various sections. Section II discusses the architecture development process including network communication protocols, topology, and bandwidth evaluation and selection. Section III presents three proposals, its evaluation, and a recommended architecture. Section IV discusses the recommended architecture's analysis and simulation. Section V summarizes and concludes.

II. Architecture development process

As an architecture development use case, the author assumes the following core electronic devices; four sensors, four display devices and one weapon station. Network architecture development for these devices involves requirements, communication protocols, network topology, and bandwidth. The evaluation process and selection rationale for each of these elements are discussed here.

A. Requirements

The architecture must meet the following requirements:

1) Secure and interoperable data handling.
2) Individual device failures shall not fail the entire network.
3) Meet military standards including information assurance.
4) Economical and simple scalability solutions.
5) Minimum logistics/maintenance footprint.
6) Reduced size, weight, and power (SWAP) consumption.

B. Communication Protocol Evaluation & Selection

A communication protocol, in a network, allows inter device interactions. Unique interfaces in the army vehicle electronics, complicates network scalability and performance. The author strongly recommends a common bus for a network to allow all devices to communicate in a standard single interface. Per author's research, the Gigabit (GB) Ethernet, CAN bus, USB 2.0, and IEEE 1394 protocols are the open standard candidates for a common bus network communication protocol.

Each of the protocols are evaluated per the factors (based

Manuscript received December 14, 2009. This work was supported in part by the Wayne State University, TARDEC under ECE5995 defense electronics project.

Macam S Dattathreya is with the Tank Automotive Research Development Engineering Center, Warren, MI 48397 USA.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **22 DEC 2009**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Open Network Architecture for Army Vehicle Electronics

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Macam S Dattathreya

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
US Army RDECOM-TARDEC 6501 E 11 Mile Rd Warren, MI 48397-5000, USA

8. PERFORMING ORGANIZATION REPORT NUMBER
20460

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)
TACOM/TARDEC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
20460

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
The army vehicle electronics networking is complex and is receiving considerable attention in the concept of open and standard architecture. Electronic devices are from multiple vendors with unique interfaces. A successful battle depends on the effective interoperable communication between these devices. No commercial open architecture available to address interoperability, scalability, and security issues. Current standard network protocols, topologies, and bandwidth requirements are evaluated, and three architecture proposals are presented and evaluated. Hardware & software service oriented open network architecture for army vehicle electronics is presented. The latency, single point failure, scalability, security, and redundancy of the proposed architecture are evaluated. Initial evaluation has shown favorable results.

15. SUBJECT TERMS
Army vehicle network architecture, electronic network architecture, open architecture, vehicle architecture

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**7**	

on author’s judgment in dealing with architectures) presented in TABLE I. In the evaluation and selection process, for each protocol, for each factor, a ranking is assigned. Each protocol’s rankings are added and the highest ranked protocol is selected.

The GB Ethernet data rate is at Gb/s (supports 1-100 Gb/s), the IEEE 1394 is at 49Mb/s, the USB is at 480Mb/s and the CAN is at 1Mb/s. The GB Ethernet and CAN has commercial hardware since 1991, the USB 2.0 since 2000, and the IEEE 1394 since 2003. All these protocols are less susceptible to hardware/software obsolescence with minimum technology risks. All are scalable except IEEE 1394. Due to low date transmission rate, the CAN is not a good video bus, but IEEE 1394 is good for video. The USB 2.0 data rate is very low compared to GB Ethernet [9].

In summary, the GB Ethernet has good data transmission rate and minimum technical risk. It is scalable and commercial networking hardware is available. Per TABLE II analysis and above evaluation, the GB Ethernet is the highest ranking protocol and the author recommends it for the common bus.

TABLE I
PROTOCOL SELECTION FACTOR AND WEIGHTING

Serial Num	Parameter	Weight (%)	Ranking weight
1	Implementation cost	8%	Low (3), Medium (2),High(1)
2	Bandwidth or throughput	22%	High(3), Medium(2), Low(1)
3	Extensibility	10%	Easy(3),Moderate (2) Complex(1)
4	Size, weight & power(SWAP)	10%	Lightest(3),Lighter (2), Light(1)
5	Commercial Availability	11%	Surplus(3),Available (2),Scarcity(1)
6	Latency	12%	Minimum(3),Medium (2), High(1)
7	Open standard/architecture	12%	Available(3),Some proprietary(2),Proprietary(1)
8	Technical risk	15%	Minimum(3),Medium(2) High(1)
	Total	**100%**	

TABLE II
PROTOCOL RANKING SUMMARY

Parameter	Gigabit Ethernet	CAN Bus	IEEE 1394	USB 2.0
Implementation cost	3* 0.08 = 0.24	3* 0.08 = 0.24	3* 0.08 = 0.24	3* 0.08 = 0.24
Bandwidth or throughput	3 * 0.22 = 0.66	1 *0.22 = 0.22	2 *0.22 = 0.44	1*0.22 = 0.22
Extensibility	3 * 0.10 = 0.30	1 * 0.10 = 0.10	1 * 0.10 = 0.10	1 * 0.10 = 0.10
Size, weight & power(SWAP)	2 * 0.10 = 0.20	2 * 0.10 = 0.20	2 * 0.10 = 0.20	3 *0.10 = 0.30
Commercial Availability	3 * 0.11 = 0.33	1 *0.11 = 0.11	3 * 0.11 = 0.33	3 * 0.11 = 0.33
Latency	3 * 0.12 = 0.36	3 * 0.12 = 0.36	1 *0.12 = 0.12	1 *0.12 = 0.12
Open source/architecture	3 * 0.12 = 0.36	3 * 0.12 = 0.36	3 * 0.12 = 0.36	3 * 0.12 = 0.36
Technical risk	3 * 0.15 = 0.45	3 * 0.15 = 0.45	3 * 0.15 = 0.45	3 * 0.15 = 0.45
Total	**2.9**	**2.04**	**2.24**	**2.02**

C. Bandwidth Analysis

In general, electronics need to process video, image and other mission critical data. The network must satisfy each data type’s bandwidth requirements.

TABLE III presents the author assumed data types, its bandwidth and frequency requirements from the assumed core devices.

To support a continuous 3 Gb/s and a frequent 0.37 Gb/s data transfer rate (per TABLE III), to reduce re acquisition cost for future expansion / scalability, the author strongly recommends a 10Gb network bandwidth and the network devices to support it.

TABLE III
BANDWIDTH ANALYSIS SUMMARY

Data type	Frequency	Date Rate
Video	Frequent	0.5 Gb/s/device
Image	Frequent	0.25 Gb/s/device
Text	Frequent	0.02Gb/s/device
Navigation	Frequent	0.12Gb/s/device
Mission Critical	Frequent	0.02Gb/s/device

D. Network Topology Evaluation & Selection

Per author’s research, a star network topology offers greater advantages over ring, mesh, tree and bus [9]. The star network is scalable and has minimal performance or operational impacts. Star networks are tolerant to single device failures. Request messages do not pass through multiple devices before reaching the target. Each device is isolated by a link that connects it to and the central hub. Multiple cable types can be used within a network.

Based on this evaluation, the author recommends a multiple star networks for device connections. Every device goes through either a router or a switch. Each device has at least two network paths to reach other devices (redundancy).

E. Network Devices Selection

TABLE IV lists the author recommended devices to develop architecture to support the core device’s operation and networking. Section III describes the details.

TABLE IV
ARCHITECTURE DEVICES

Data type	Comments
Storage	For data storage.
Master computers	For data handling
Routers	For data routing between networks.
Switches	For creating a network
Gateways	For protocol conversions.
Common time module	For synchronized time across the network.

III. ARCHITECTURE PROPOSAL PROCESS

The proposal process consists of developing alternate architectures and their evaluation, and a recommended architecture.

A. Architecture Proposals

Author, developed several alternative architecture proposals to satisfy the requirements defined in the section II A. All alternatives had similar organization, but only three best were selected for the final evaluation.

Proposal#1 (P1) (Fig. 1) recommends a separate 10 Gb Ethernet star network per data classification to secure data handling and to restrict any cross contamination between them. The separate network minimizes complicated data handling software and bandwidth contention. In this proposal, to support the use case established in section II, the author recommends the following:

1) At least two communication paths between devices to minimize single point failures.
2) Two Ethernet switches to form a redundant network per data classification.
3) Three Gateway devices for protocol conversions and redundancy.
4) One central computer per network for data handling.

P1 has the following high level limitations:

1) Increased devices due to separate networks create vehicle clutter and complicate maintenance.
2) Increased SWAP issues.

Proposal#2 (P2) (Fig. 2) recommends 10 Gb Ethernet star network with a combined hardware and software data handling solution. In addition to hardware elements, this proposal recommends Service Oriented Architecture (SOA) software components for data collection, data processing, data storing, data security and data distribution. In this proposal, to support the use case established in section II, the author recommends the following:

1) At least two communication paths between devices to minimize single point failures.
2) Three Ethernet switches to form a redundant network.
3) Two routers with built in firewalls and network management software to connect Ethernet switched networks and any other devices.
4) Three Gateway devices for protocol conversions and redundancy.
5) One central data storage device, two vehicle master computers for data handling and to provide load balancing.
6) Centralized SOA based data handling software.

P2 has the following high level limitations:

1) Requires complex configuration and secure data handling software.
2) More Ethernet Switches required if more number of devices need to be added. This creates SWAP issues.

Proposal#3 (P3) (Fig. 3) recommends a modified P2 with reduced number of network devices and wiring. This proposal recommends redundancy at the Ethernet switch level and minimizes SWAP issues. In this proposal, to support the use case established in section II, the author recommends the following:

1) At least two communication paths between Ethernet switches to minimize single point failures.
2) Four Ethernet switches to form a redundant network.
3) Two Gateway devices for protocol conversions and no additional redundant device.
4) One central data storage device, two vehicle master computers for data handling and to provide load balancing.
5) Centralized SOA based data handling software.
6) Secure data transmission with no data contamination between multiple data classifications.

P3 has the following high level limitations:

1) Display devices have to hop through three switches to reach sensors. This has additional latency.
2) The redundancy is at the Ethernet switch level and if a device link to switch is broken, the device will be off line.

B. Architetcure Proposals Analysis

Each of the three proposals is evaluated using the following factors.

1) Data Security (Information Assurance)
2) Redundancy
3) Single point failures
4) Size, weight & power consumption(SWAP)
5) Scalability

Each factor is given a ranking 1- 3 (1 is the lowest). The P1 recommends separate network per data classification and provide highest data security. The P2 and P3 recommend software based highest data security. The P1 creates maintenance and SWAP complexities. The software based security allows more control with less maintenance and SWAP complexities. *Per this rationale, the P1, for data security, ranks as 2, P2 and P3 ranks as3.*

The P1 recommends redundant network per data classification, which requires more network devices. The P2 recommends redundant networks and the chances of adding more devices are slim unless huge number of devices is added to the network. The P3 recommends redundancy at the Ethernet switch level and if a device link to the switch is broken, the device will be off the network. *Per this rationale, the P1, for redundancy, ranks as 2, P2 ranks as 3, and P3 ranks as 1.*

The P1and P2 recommends redundancy at both the Ethernet switch and the device level, which contributes to minimal single point failures. The P3 recommends redundant links at the Ethernet switch level; this contributes to more single point failures for devices. *Per this rationale, for single point failures, the P1 & P2 ranks as 3 and P3 ranks as 1.*

The P1 recommends redundant network per data classification, which creates additional number of network devices which contributes to SWAP issues. The P2 recommends redundant network at both Ethernet switch and device level and does not recommend more switches. It still contributes some SWAP issues. The P3 proposes very minimal Ethernet level redundancy and recommends minimal network devices. The P3 contributes size, very minimal SWAP issues. *Per this rationale, for SWAP, the P1 ranks as 1, P2 ranks as 2 and P3 ranks as 3.*

The P1 is scalable but it complicates the network, adds too much clutter in the vehicle, and the maintenance is complicated too. The P2 and P3 shares the same scalability issues as P1, but to a less degree due to the software based data security features. *Per this rationale, for scalability, the P1 ranks as 1, P2 and P3 ranks as 2.*

Each proposal's rankings are added and the architecture with the highest ranking is the best candidate. The P2 has the highest ranking of 15. The author recommends P2 as the best architecture proposal among the three alternatives.

C. Recommended Architecture

Army vehicle is used for creating force and moving infantry to battlefield quickly. The vehicle operates in different terrains. The electronics on this vehicle continuously monitor and feed mission critical information to the crew. Each vehicle will have electronic devices and weapons to carry out missions. For an effective operation of these devices, a solid, fault tolerant network is needed. The Fig. 4 shows the recommended architecture diagram.

The sensors continuously or on demand capture data. The data is displayed, processed, distributed, and stored. The captured data enables crew members to take actions and eliminate enemy forces using on board weapons. The section III A describes the recommended architecture briefly. In this section, the author describes the details.

In addition to hardware elements, author recommends SOA based software components for data collection, data processing, data store, data security, and data distribution. This paper discusses high level software details and does not provide any low level implementation, logic or code details. The author recommends two 10Gb Ethernet router networks with three 10Gb Ethernet switch networks for fault tolerance and reduced single point failures. He proposes physical connection schemes (refer Fig. 4) for sensors, displays, weapon station, storage, and computer resources.

The sensor network connections allow continuous or on demand data capture. Sensors are connected to two router networks, which provide high availability and redundancy. They minimize single point failures. Ethernet switch allows easy expansion of additional sensors. If any one of the network channels is broken, the sensors can be accessed via available redundant channels. Gateways are used for protocol conversions (CAN to Ethernet). The router connections allow other devices to interact with sensors.

The display devices network allows continuous or on demand data capture from sensors and vehicle master computer. Displays are connected to two router networks which provide high availability and redundancy. They minimize single point failures. Ethernet switch#2 allows easy expansion of additional display devices. If any one of the network channels is broken, the displays can access the network via available redundant channel. Gateways are used for protocol conversions (USB to Ethernet). The router connections allow these devices to interact with sensors, weapon station and vehicle master computer.

Weapon station is capable of operating on its own without a network resource. A weapon station does not need many redundant channels.

The vehicle computers are the master processing power for data recording, processing, storage, and distribution. The storage device is the media captured data storage. The recommended physical connection allows these devices to access sensors, displays and weapon stations. The network provides redundant channels to access other devices. The author recommends using two computers for load balancing and a common time module for synchronized time across the network.

The author recommends SOA software components for data capturing, processing, storing and distributing. These components are developed using C++ or Java. The display device's software provides human factors engineered user interfaces. The display devices are the clients, and the vehicle master computers are the service providers for the requested data. The display devices have the capability to interact with any devices in the network with proper access controls.

The author recommends two types of sensor data capturing mechanisms i.e. batch mode (automatic) and user initiated. The user initiated capture client software resides in all the onboard display devices. The client interfaces with the service software in the master computer. The client component will have a display device specific unique id. Crew members request sensor data using client software's controls. The client software executes a request for data from the service running on the master computer. The request input will have the user id, password, sensor type, and the unique id. The request will be accepted by the service software and is validated. If the requested sensor is a secure data, the service software validates the access authority and then fulfils the request. The data will be sent to the display device and then it is stored in the central storage for playback later. The batch (automatic) capture service software running on the master computer, automatically captures all the sensors data continuously and stores in the central storage for later playback.

The data processing software resides in the vehicle master computer. It is invoked when display controls issue appropriate commands to execute a specific function. It validates user credentials, encrypt data, and provide processing modules for data distribution, storage, compression, validation, event logging, sensor data recording, executing weapon controls, and etc. This software controls the data distribution and data storage software modules.

The data distribution software resides in the vehicle master computer. It is invoked by the data processing software to delegate data distribution function. It takes care of all the controls and algorithms to distribute data between the various displays and the sensor devices. It provides mechanisms for secure and controlled data distribution.

The data storage software resides in the vehicle master computer. It is invoked by the data processing software. The data storage software takes care of all the controls and algorithms to compress, encrypt, and store data. It provides secure and controlled mechanisms for storing data to the central storage. The software encrypts data prior to storing.

IV. Analysis And Simulation

In a network, as the bus traffic increases, the queuing delay for the messages to get the bus increases. If *u* is the utilization of a particular bus, then the probability that a message will get the bus during its first trial is $(1 - u)$. The probability that the message will not get the bus during its first trial but will get the bus during its second trial is $u(1 - u)$. In general, the probability that the message will not get the bus during the first $(i - 1)$ trials but it will get the bus during the *i*th trial is $u^{i-1}(1 - u)$. Hence, the average number of trials necessary for the message to get the bus is 1/(1-u) [2].

The average message transmission delay through the bus, including the queuing delay for the bus, is $l_{avg/}\ ((1-u)BW_{)}$. Where, l_{avg} is the average length of a message and *BW* is the bandwidth of the bus [2]. The average message transmission delay for the bus including the queuing delay for the bus is $ul_{avg/}\,((1-u)BW_{)}$

For a particular message, the end-to-end latency due to network components, such as buses, switches, routers and gateway devices, can be expressed as:

$$T = T_{bs} + T_{sw} + T_{gd} + T_{rtr} \qquad (1)$$

where, T_{bs} is the source bus delay; T_{sw} is time required by the source switch device ; T_{gd} is time required by the gateway devices to convert messages from one protocol to another protocol; T_{rtr} is time required by the source router devices. The time for switches, routers and gateway devices increases if the number of these devices increases.

The author recommends an average 30% primary bus utilization to allow future expansions. In the recommended architecture, if the primary link is broken, the redundant network path is used. In this architecture, the network performance degrades if multiple links are faulty in a given network segment. The big latency in this architecture is from the Ethernet switches, routers and gateway devices.

The bottleneck instances are very minimal in this architecture. In this section, author analyzes the device performance using mathematical models defined earlier in this section. For discussion purposes, consider the following three separate instances of faulty primary paths.

1) **Instance1**: Link#2 is broken (refer Fig. 4)
2) **Instance2:** Link#5 is broken(refer Fig. 4)
3) **Instance3:** Link#10 is broken (refer fig. 4)

For analysis purpose, assume the following:

1) One Ethernet switch has a latency of 2 milliseconds.
2) One Ethernet router has a latency of 3 milliseconds.
3) One Gateway device has a latency of 2 milliseconds.
4) The bus utilization on the link#1 is 20%, link#2 is 30%, link#3 is 30%, link#5 is 20%, link#6 is 20%, link#7 is 30%, link#8 is 40%, link#9 is 20% and link#10 is 10%.

During normal operation via Link#2, the bus utilization is 30% and the bus latency for a 0.5Gb length data from sensor1 is calculated as follows: 0.5/((1-0.3)10) = 0.0714milliseconds. The total end to end time for a normal message transfer is calculated based on the equation (1). The total time = 0.0714 + 3 + 2 = 5.0714 milliseconds (from one switch and one router).

If the Link#2 is faulty, then the network traffic uses Link#6 as a next best route, this creates additional load on it, now the Link#6 utilization is increased by 30% more. Now the Link#5 bus utilization is 50%. The bus delay for sensor1 data on this link is 0.5/((1-0.5)10) = 0.1milliseconds. The total end to end time for this message transfer on the alternate path is calculated based on the equation (1). The total time = 0.1 + 3 + 2 = 5.1 milliseconds (from one switch and one router).

Based on the content from this sensor, the user initiates appropriate action e.g. use a weapon station to fire or store the video content to the master computer. In a hostile condition, if the target is moving fast towards the vehicle, the user needs the sensor data at the display device within the expected X milliseconds. If X < 5.1 milliseconds then both the primary and alternate paths are good links else appropriate analysis needs to be done to improve the performance of a link which is >X.

During normal operation via Link#5 the bus utilization is 20% and the bus delay for a 0.01.Gb length data from sensor2 is: 0.01/ ((1-0.2)10) = 0.00125milliseconds. The total end to end time for a normal message transfer is 0.00125 + 2 + 3 = 5.00125 milliseconds (from one gateway and one router).

If the Link#5 is faulty, Link#7+Link6 path is used. The Link#7 bus delay, for 0.01Gb data length, based on 30% + 20% (from faulty link traffic) bus utilization is 0.002 milliseconds. The Link#6 bus delay due to 20% additional bus utilization is 0.0025. The total end to end time for the message transfer on the alternate path is 0.002+ 0.0025 + 2 + 3 + 2 = 7.0045 milliseconds (from one gateway, one switch and one router).

Based on the sensor2 data, the user initiates necessary steps to avoid collision or attack. The display expects sensor data within X milliseconds. If X <7.005 milliseconds, then both primary and alternate paths are good, else appropriate analysis needs to be done to improve performance of a link which is >X.

During normal operation via Link#10 + Link#2, weapon station is controlled from Display 1or 2 or 3. The bus delay on Link#10 from its 10% bus utilization is 0.0011 to transfer 0.01 Gb data. The bus delay from Link#2 is 0.0714 milliseconds.

The total end to end time on this path is = 0.0011 + 0.0714 + 2+ 3 = 5.0725 milliseconds.

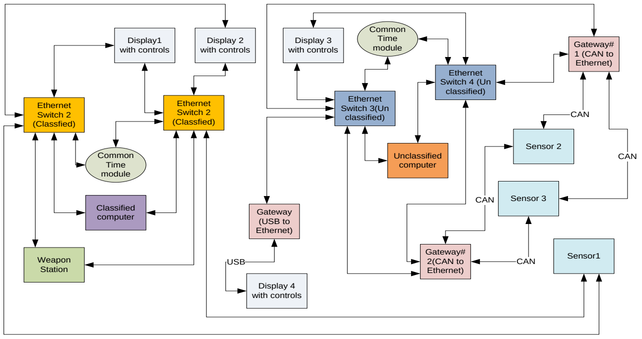

Fig. 1. Architecture proposal#1

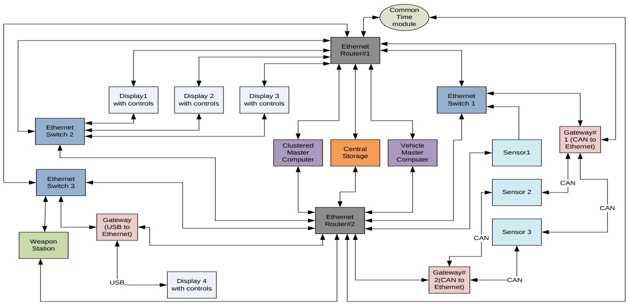

Fig. 2. Architecture proposal#2

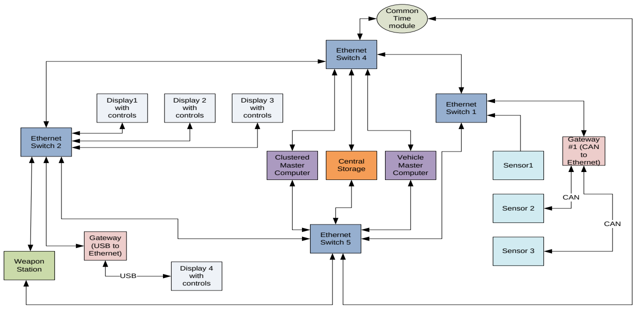

Fig. 3. Architecture proposal#3

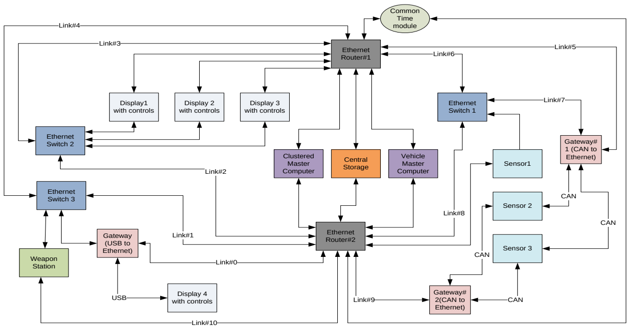

Fig. 4. Recommended network architecture for army vehicle electronics

If the Link#10 is broken and the communication takes Link#2+Link#1 path. Now, bus delay on Link#1 due to 20% + 10% is 0.00143milliseconds. The total end to end time for the message transfer on the alternate path is 0.0714 + 0.00143 + 2 + 3 + 2 = 7.0728 milliseconds (from two switches and one router).

Based on the display data, the weapon station initiates necessary attack. The station expects display data within X milliseconds. If X <7.0728 milliseconds, then both primary and alternate paths are good, else appropriate analysis needs to be done to improve performance of a link which is >X.

The average message transmission delay for the bus including the queuing delay for the bus in Link#2 (at 30% bus utilization) is 0.0714 *0 .3 = 0.0214 milliseconds. If additional load added to it during fault conditions, the bus delay increases.

The average message transmission delay for the bus including the queuing delay for the bus in Link#7 (at 50% bus utilization) is 0.002 * 0.5 = 0.01milliseconds. If additional load added to it during fault conditions, the bus delay increases.

V. Conclusion

The author recommended architecture uses standard technologies and promotes open architecture standards. The 10Gb Ethernet data bus for this network are faster, scalable, and is capable of handling at least five additional sensors and displays. The recommended network devices are optimal and they minimize SWAP allocations. The common data bus approach promotes easy expansion, provides good interoperable solution, and is compliant with the military standards. The built in firewalls and network management software on router devices reduce risks and development costs.

The author recommended SOA software modules control the data security and distribution between devices.

The author recommended architecture can be implemented on any army ground vehicles with minimum modifications. It enables successful battle mission with high availability and faster data transfer. In this architecture, the data is secure and the access is restricted to the authorized personnel. The recommended technologies are less susceptible to hardware/software obsolescence.

Author does not recommend any vendor specific products and promotes economical procurement.

Acknowledgment

Macam S Dattathreya wishes to thank Dr. Mahmud and Dr. Singh of Wayne State University for their support. He also wishes to thank Pame Watts of TARDEC University dean for her support. He also wants to thank Mark Slominski, Philip Smith, Eric Bennett and Doug Gersky of TARDEC-SEC for their review support for this paper.

Disclaimer

Disclaimer: Reference herein to any specific commercial company, product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the Department of the Army (DoA). The opinions of the authors- expressed herein do not necessarily state or reflect those of the United States Government or the DoA, and shall not be used for advertising or product endorsement purposes.

REFERENCES

[1] Rabadi, N. M., & Mahmud, S. M. (2007). "Privacy Protection among Drivers in Vehicle-to-Vehicle Communication Networks", Proceedings of the 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, January 11-13, 2007.

[2] S. M. Mahmud, "In-Vehicle Network Architecture for the Next-Generation Vehicles," Chapter XV, *Wayne State University, Detroit*, MI, pp. 281–294.

[3] "*DoD Architecture Framework Version 1.5"*, "Net centric guidance for architecture product section, April 23, 2007, pp.31 – 37.

[4] P. Ross, "Information Assurance (IA) in the Defense Acquisition System," *Department of Defense INSTRUCTION.*, Information Assurance (IA) Implementation, DODI 8500.2, February 6, 2003., pp. 30–35.

[5] "Multiple Independent Levels of Security/Safety (MILS) ". [Online]. Available:http://www.ois.com/Products/MILS-Technical-Primer.html.

[6] "Network Protocols Handbook by Jawin Technologies", Edition: 2 - 2005, pp-11-32, pp-146-148.

[7] Chris McNab (Oreilly), Edition: 1, "Network Security Assessment" , March 2004.

[8] "System of systems common operating environment (SOSCOE)," Boeing *News, pp. 37-57*.

[9] Online].http://en.wikipedia.org/wiki/List_of_network_protocol.

[10]]"Network architecture fundamentals".[Online]. Available:http://www.informit.com/articles/article.aspx?p=21260&rll=1 .

Macam S. Dattathreya received B.E degree in Industrial and Production Engineering from the University of Mysore, India in 1994, and the M.S degree in Computer Engineering from the Wayne State University, Detroit, MI, USA in 1999.

He was with IBM global services as a lead IT architect from 1999 to 2009, where he filed seven software patents and published three technical journals.